Document Owner:
Effective Date:
Updated:

Incident response policy

[Company Name]

|  |
| --- |
| **[Company Name]****Incident Response Policy** |
| **Effective Date:** |  | **Document Owner:** |  |
| **Revision History** |
| Revision | Rev. Date | Description | Prepared By | Reviewed By | Date | Approved By | Date |
| 1.0 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

[1. Purpose 1](#_Toc11665117)

[2. Scope 2](#_Toc11665118)

[3. Policy 2](#_Toc11665119)

[3.1 Confirmed Theft, Data Breach, or Exposure of Protected or Sensitive Data 2](#_Toc11665120)

[3.2 Ownership and Responsibilities 3](#_Toc11665121)

[3.3 Communication Plan 3](#_Toc11665122)

[3.4 Incident Reporting 3](#_Toc11665123)

[3.5 Incident Mitigation 3](#_Toc11665124)

[3.6 Incident Analysis Process 4](#_Toc11665125)

[3.7 Policy Review 4](#_Toc11665126)

[4. Enforcement 4](#_Toc11665127)

[5. Related Standards, Policies, and Processes 4](#_Toc11665128)

[6. Relevant Subcontrols 4](#_Toc11665129)

[7. Definitions and Terms 4](#_Toc11665130)

# Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. Response processes and procedures must be executed and maintained, to ensure response to detected cybersecurity incidents.

<Company> Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how <Company>’s established culture of openness, trust and integrity should respond to such activity. <Company> Information Security is committed to protecting <Company>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach or exposure of <Company> Protected data or <Company> Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@<Company>.org, by calling 555-1212, or using the help desk reporting web page at http://<Company>. This e-mail address, phone number, and web page are monitored by the <Company>’s Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

# Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of <Company> members. Any agreements with vendors will contain language similar that protects <Company>.

# Policy

## Confirmed Theft, Data Breach, or Exposure of Protected or Sensitive Data

As soon as a theft, data breach or exposure containing <Company> Protected data or <Company> Sensitive data is identified, the incident response process will begin either during or after the incident. All access to the compromised resource should be removed.

The Executive Director will chair an incident response team to handle the breach or exposure. The team will include members from:

* IT Infrastructure
* IT Applications
* Finance (if applicable)
* Legal
* Communications
* Member Services (if Member data is affected)
* Human Resources
* The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
* Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

## Ownership and Responsibilities

* Sponsors - Sponsors are those members of the <Company> community that have primary responsibility for maintaining any information resource. Sponsors may be designated by any <Company> Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
* Information Security Administrator is that member of the <Company> community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
* Users include virtually all members of the <Company> community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
* The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

## Communication Plan

* Following an incident, work with <Company> communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected. Information sharing must occur with external stakeholders to notify them following an incident. The information sharing and coordination with stakeholder should occur consistent with the following requirements:
	+ <INSERT INFORMATION SHARING AND STAKEHOLDER COORDINATION PLAN>

## Incident Reporting

All incidents should be reported immediately and in a manner with the following established criteria.

* <INSERT REQUIRED CRITERIA>

## Incident Mitigation

The following activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

* <INSERT MITIGATION ACTIVITIES>

New vulnerabilities identified in the risk management process should be mitigated through the activities outlined above or document as accepted risks.

## Incident Analysis Process

Following cybersecurity incidents, analysis is conducted to ensure effective response and support recovery activities. The analysis should follow these steps:

1. Document the impact of the incident.
2. Perform forensics.
3. Categorize the incident

## Policy Review

The organizational response plan should be reviewed after each incident to make improvements. The review should incorporate lessons learned from current and previous detection/response activities. This review should also include perspectives from internal and external stakeholders.

# Enforcement

Any <Company> personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

# Related Standards, Policies, and Processes

* Risk Management Policy
* Disaster Recovery Plan
* Access Control Policy

# Relevant Subcontrols From the NIST CSF (v1.1) Framework

|  |  |
| --- | --- |
| **Name** | **Identifier** |
| Response Communications | RS.CO-1 to RS.CO-5 |
| Response Analysis | RS.AN-1 to RS.AN-5 |
| Incident Mitigation | RS.MI-1 to RS.MI-3 |
| Response Improvements | RS.IM-1 to RS.IM-2 |

# Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

|  |  |
| --- | --- |
| **Term** | **Definition** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |